Polynomial Interpolation of the Naor-Reingold Pseudo-Random Function

Thierry Mefenza, Damien Vergnaud

Appl. Algebra Engrg. Comm. Comput. manuscript No.
(will be inserted by the editor)

Polynomial Interpolation of the Naor-Reingold Pseudo-Random Function

Thierry Mefenza · Damien Vergnaud

Received: date / Accepted: date

Abstract We prove lower bounds on the degree of polynomials interpolating the Naor-Reingold Pseudo-random Function over a finite field and over the group of points on an elliptic curve over a finite field.

Keywords Naor-Reingold pseudo-random function · polynomial interpolation · finite fields · elliptic curves.

MSC Codes 11T71,94A60

1 Introduction

In cryptography, a pseudo-random function family is a collection of functions (that can be evaluated efficiently using a secret-key) with the property that an adversary cannot efficiently observe any significant difference between the input-output behavior of a random instance of the family or that of a random function.

More formally, we consider collections of functions $\{F_n : \mathcal{K}_n \times \mathcal{D}_n \rightarrow \mathcal{R}_n\}_{n\in\mathbb{N}}$ that can be evaluated by a (deterministic) polynomial-time Turing Machine. We define an adversary as a (non-uniform) probabilistic polynomial-time oracle Turing machine with either access to:

The authors are supported in part by the French ANR JCJC ROMAnTIC project (ANR-12-JS02-0004) and by the Simons foundation Pole PRMAIS.

T. Mefenza
Département d'informatique, École normale supérieure, 45 rue d'Ulm, F-75230 Paris Cedex 05, France Department of Mathematics, University of Yaounde 1, Cameroon. E-mail: mefenza@di.ens.fr

D. Vergnaud
Département d'informatique, École normale supérieure, 45 rue d'Ulm, F-75230 Paris Cedex 05, France. E-mail: damien.vergnaud@ens.fr

- an oracle implementing a function $F : \mathcal{D}_n \to \mathcal{R}_n$ defined by picking uniformly at random a secret-key $k \in \mathcal{K}_n$ such that $F(m) = F_n(k, m)$ for any $m \in \mathcal{D}_n$;
- or an oracle simulating a truly random function $F : \mathcal{D}_n \to \mathcal{R}_n$ (*i.e.* whose outputs are sampled uniformly and independently at random).

This adversary can decide which queries to make to the oracle, perhaps based on answers received to previous queries and eventually, it outputs a single bit (which is its decision as to which function the oracle is implementing). The *advantage* of the adversary is the function of n defined as the difference of the probabilities (taken over the random choices made by the adversary and the oracle) that the adversary outputs 1 in the two cases. A collection of functions $\{F_n : \mathcal{K}_n \times \mathcal{D}_n \to \mathcal{R}_n\}_{n\in\mathbb{N}}$ is a pseudo-random function family if and only if no adversary with advantage asymptotically larger than the inverse of a polynomial exists.

In 1997, Naor and Reingold [16,17] proposed a (candidate) pseudo-random function family which takes inputs in $\{0,1\}^n$ (for some parameter n) and outputs an element in some (multiplicatively written) group $\mathbb{G}$ of prime order ℓ with generator g. The secret key is an n-dimensional vector $\mathbf{a} = (a_1, \ldots, a_n) \in ((\mathbb{Z}/\ell\mathbb{Z})^*)^n$ and the Naor-Reingold function is defined as:

$$\begin{aligned} f_{\mathbf{a}} : \quad \{0,1\}^n &\longrightarrow \mathbb{G} \\ (x_1, \ldots, x_n) &\longmapsto f_{\mathbf{a}}(x_1, \ldots, x_n) = g^{\prod_{i=1}^{n} a_i^{x_i} \bmod \ell} \end{aligned}$$

The evaluation of $f_{\mathbf{a}}$ is thus efficient[1] since it consists only in n modular multiplications in $\mathbb{Z}/\ell\mathbb{Z}$ and one modular exponentiation in $\mathbb{G}$. To lighten the notation, given an n-dimensional vector $\mathbf{a} = (a_1, \ldots, a_n) \in ((\mathbb{Z}/\ell\mathbb{Z})^*)^n$ and a variable x that will denote indifferently an n-bit string $(x_1, \ldots, x_n) \in \{0,1\}^n$ or an integer $x \in \{0, 1, \ldots, 2^n - 1\}$ (which implicitly defines $(x_1, \ldots, x_n) \in \{0,1\}^n$ the bit representation of x with extra leading zeros if necessary), we denote $\mathbf{a}^x$ the element in $\mathbb{F}_\ell$ defined by $\mathbf{a}^x = a_1^{x_1} \cdots a_n^{x_n} \bmod \ell$. With this notation, the Naor-Reingold function is simply defined by $f_{\mathbf{a}}(x) = g^{\mathbf{a}^x}$.

It is shown in [16,17] that the Naor-Reingold function is pseudo-random provided that certain standard cryptographic assumptions about the hardness of breaking the Decision Diffie-Hellman assumption holds. In cryptography, two interesting choices for $\mathbb{G}$ are a subgroup of the multiplicative group of a (prime) finite field and a subgroup of the points of an elliptic curve defined over a finite field.

Since proving that the Decision Diffie-Hellman assumption holds seems currently to be out of reach, several number-theoretic properties and complexity measures have been studied for the Naor-Reingold pseudo-random functions over finite fields as well as over elliptic curves: distribution (see [14,19] and references therein), linear complexity (see [5,6,18,20]) and non-linear complexity

[1] More efficient candidates of pseudo-random function families are known, but the Naor-Reingold function family is among the most efficient ones with strong security guarantees under a standard computational assumption.

(see [1]). These results are incomparable but they all support the assumption of the pseudo-randomness of the Naor-Reingold function.

In order to break the security of the Naor-Reingold function, it would be sufficient to have a polynomial over a finite field of low degree which reveals information on the function values. From the known lower bounds on the polynomial interpolation on the discrete logarithm in the groups we considered (*e.g.* [4,10–12,15])), it is easy to prove that a low-degree t-variate polynomial cannot reveal the secret key $\mathbf{a}$ when evaluated at $f_{\mathbf{a}}(x^{(1)})$, $f_{\mathbf{a}}(x^{(2)})$, $\ldots$, $f_{\mathbf{a}}(x^{(k)})$ (for integers $x^{(1)}, \ldots, x^{(k)} \in \{0, 1, \ldots, 2^n - 1\}$) for many different vectors $\mathbf{a}$. However, the security of the Naor-Reingold function would be broken if such low-degree polynomial revealing a value $f_{\mathbf{a}}(x^{(0)})$ were proved to exist (for some integer $x^{(0)} \in \{0, 1, \ldots, 2^n - 1\} \setminus \{x^{(1)}, \ldots, x^{(k)}\}$).The reduction of the Naor-Reingold function pseudo-randomness to the Decision Diffie-Hellman problem uses a so-called *hybrid argument* and known lower bounds on the polynomial interpolation on the Diffie-Hellman mapping (*e.g.* [9,7,13,22])) are not strong enough to rule out the existence of such polynomials for $k > 2$.

The present article deals with the polynomial representation of the Naor-Reingold function over finite fields and elliptic curves and proves lower bounds on the degree of polynomials which interpolate these functions. Our results are of the following form: for most secret keys $\mathbf{a}$, if a multivariate polynomial reveals the value $f_{\mathbf{a}}(x^{(0)})$ when evaluated at values $f_{\mathbf{a}}(x^{(0)} + t_1)$, $f_{\mathbf{a}}(x^{(0)} + t_2)$, $\ldots$, $f_{\mathbf{a}}(x^{(0)} + t_k)$ for fixed values $t_1, \ldots, t_k$ and for many integers $x^{(0)} \in \{0, 1, \ldots, 2^n - 1\}$, then this polynomial is of high degree. We consider univariate, bivariate and general multivariate polynomial representation of the Naor-Reingold function. These lower bounds do not have any immediate implications for the pseudo-randomness of the Naor-Reingold function but as the results mentioned above they support this assumption. In particular, the inverse statements of the existence of low degree polynomial representation of the function would completely break the security of many cryptographic schemes.

2 Preliminaries

Throughout the paper, $\log z$ denotes the binary logarithm of z. Let p be an odd prime number. We denote by $\mathbb{F}_p$ the finite field with p elements and the elements of $\mathbb{F}_p$ are identified with the set of integers $\{0, \cdots, p-1\}$. Given $g \in \mathbb{F}_p^*$ with prime order ℓ (with $\ell \mid p-1$) we can consider the Naor-Reingold pseudo-random function defined over $\mathbb{G} = \langle g \rangle$: $f_{\mathbf{a}}(x) = g^{\mathbf{a}^x} \in \mathbb{G} \subset \mathbb{F}_p^*$, for a secret key $\mathbf{a} = (a_1, \ldots, a_n) \in (\mathbb{F}_\ell^*)^n$ where x will denote indifferently an n-bit string $(x_1, \ldots, x_n) \in \{0,1\}^n$ or an integer $x \in \{0, 1, \ldots, 2^n - 1\}$.

In the following, we will use the following lemma where the *weight* $w(F)$ (or sparsity) of a polynomial $F(X) \in \mathbb{F}_p[X]$ is the number of its non-zero coefficients.

Lemma 1 ([11]) *Let $\gamma \in \mathbb{F}_p$ be an element of order ℓ and $F(X) \in \mathbb{F}_p[X]$ be a non-zero polynomial of degree at most $\ell - 1$ with at least b zeros of the form γ^x with $0 \leq x \leq \ell - 1$. The weight of $F(X)$ satisfies*

$$w(F) \geq \frac{\ell}{\ell - b}$$

We will also consider the setting of an elliptic curve E defined over $\mathbb{F}_p$ for $p > 3$, that is a rational curve given by the following Weierstrass equation

$$y^2 = x^3 + Ax + B, \quad A, B \in \mathbb{F}_p, \quad 4A^3 + 27B^2 \neq 0.$$

The set $E(\mathbb{F}_p)$ of the points of the curve defined over $\mathbb{F}_p$ (including the special point O at infinity) has a group structure (denoted additively) with an appropriate composition rule where O is the neutral element. Given P a point of the curve E with prime order ℓ (with $\ell \mid \#E(\mathbb{F}_p)$), we denote $[r]P$ the scalar multiplication, i.e. in fact the adding of the point P to itself r times (for $n \geq 0$):

$$[r]P = \underbrace{P + \cdots + P}_{r \text{ times}}$$

(and $[r]P = -([-r]P)$ for $r \leq 0$). We also define the function $\tilde{f}_{\mathbf{a}}(x) = [\mathbf{a}^x]P \in E \subset \mathbb{F}_p^2$, for a secret key $\mathbf{a} = (a_1, \ldots, a_n) \in (\mathbb{F}_\ell^*)^n$ where again x will denote indifferently an n-bit string $(x_1, \ldots, x_n) \in \{0,1\}^n$ or an integer $x \in \{0, 1, \ldots, 2^n - 1\}$. Because of the algebraic structure of E, this function is not pseudo-random and the Naor-Reingold pseudo-random function over $E(\mathbb{F}_p)$ is thus defined as, $f_{\mathbf{a}}(x) = X(\tilde{f}_{\mathbf{a}}(x))$, where $X(P)$ denotes the abscissa of $P \in E$.

We recall some basic facts on division polynomials of elliptic curves (see [21] and [2]). They provide a way to calculate multiples of points on elliptic curves. The *division polynomials* $\psi_m(X, Y) \in \mathbb{F}_p[X, Y]/(Y^2 - X^3 - AX - B)$, $m \geq 0$, are recursively defined by:

$$\begin{aligned}
\psi_0 &= 0 \\
\psi_1 &= 1 \\
\psi_2 &= 2Y \\
\psi_3 &= 3X^4 + 6AX^2 + 12BX - A^2 \\
\psi_4 &= 4Y(X^6 + 5AX^4 + 20BX^3 - 5A^2X^2 - 4ABX - 8B^2 - A^3) \\
\psi_{2m+1} &= \psi_m + 2\psi_m^3 - \psi_{m-1}\psi_{m+1}^3, \quad m \geq 2 \\
\psi_{2m} &= \psi_m(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2)/\psi_2, \quad m \geq 3,
\end{aligned}$$

where ψ_m is an abbreviation for $\psi_m(X, Y)$. If m is odd, then $\psi_m(X, Y) \in \mathbb{F}_p[X]$ is univariate and if m is even then $\psi_m(X, Y) \in \psi_2(X, Y)\mathbb{F}_p[X] = 2Y\mathbb{F}_p[X]$. Therefore, as $\psi_2^2(X, Y) = 4(X^3 + AX + B)$, we have $\psi_m^2(X, Y) \in \mathbb{F}_p[X]$ and $\psi_{m-1}(X, Y)\psi_{m+1}(X, Y) \in \mathbb{F}_p[X]$. In particular, we may write $\psi_{2m+1}(X)$ and $\psi_m^2(X)$.

As mentioned above, the division polynomials can be used to calculate multiples of a point on the elliptic curve E. Let $P = (x, y) \in E$ with $P \neq O$, then the abscissa of $[m]P$ if $[m]P \neq O$ is given by

$$\frac{\theta_m(x)}{\psi_m^2(x)}, \quad \text{where } \theta_m(X) = X\psi_m^2 - \psi_{m-1}\psi_{m+1}.$$

The zeros of the denominator $\psi_m^2(X)$ are exactly the first coordinates of the non-trivial m-torsion points, i.e, the points $Q = (x, y) \in \overline{\mathbb{F}_p}^2 \setminus \{O\}$ on E with $[m]Q = O$. Note, that these points occur in pairs $Q = (x, y)$ and $-Q = (x, -y)$, which coincide only if $2Q = O$, i.e, if x is a zero of $\psi_2^2(X)$.

We recall that the group of m-torsion points $E[m]$, for an elliptic curve E defined over a field of characteristic p, is isomorphic to $(\mathbb{Z}/m\mathbb{Z})^2$ if $p \nmid m$ and to a proper subgroup of $(\mathbb{Z}/m\mathbb{Z})^2$ if $p \mid m$. If m is a power of p then $E[m]$ is either isomorphic to $(\mathbb{Z}/m\mathbb{Z})$ or to $\{O\}$. Accordingly, the degree of $\psi_m^2(X)$ is $m^2 - 1$ if $p \mid m$ and strictly less than $m^2 - 1$ otherwise. In particular, for $p = 2$ and m a power of 2 we have $\deg(\psi_m^2) = m - 1$ if E is not supersingular and $\deg(\psi_m^2) = 0$ otherwise. By induction one can show that $\theta_m(X) \in \mathbb{F}_p[X]$ is monic of degree m^2.

In the following, we will make use of the two following technical lemmas (where $\overline{\mathbb{F}_p}$ denotes as usual the algebraic closure of $\mathbb{F}_p$).

Lemma 2 *Let $E : y^2 = x^3 + Ax + B$ be an elliptic curve over $\mathbb{F}_p$ with $A \neq 0$ and $B \neq 0$. Let $F(X) \in \mathbb{F}_p[X]$ be a non-constant polynomial with $F(X) \neq X$ and $\deg(F) < p$. Then there exists $\alpha \in \overline{\mathbb{F}_p}$ such that $\psi_2^2(F(\alpha)) = 0$ and $\psi_2^2(\alpha) \neq 0$.*

Proof There are exactly three distinct zeros $\alpha_1, \alpha_2, \alpha_3 \in \overline{\mathbb{F}_p}$ of $\psi_2^2(X)$. For all index $i \in \{1, 2, 3\}$, there exists at least one $\beta_i \in \overline{\mathbb{F}_p}$ such that $F(\beta_i) = \alpha_i$, because F is not a constant polynomial. Since for all $i, j \in \{1, 2, 3\}$, $i \neq j$, we have $\alpha_i \neq \alpha_j$, then the system $F(X) = \alpha_i$ and $F(X) = \alpha_j$ has no solution. It follows that the polynomial $\psi_2^2(F(X))$ has at least three different zeros.

Let $d < p$ denote the degree of F and let us suppose that there does not exist $\alpha \in \overline{\mathbb{F}_p}$ such that $\psi_2^2(F(\alpha)) = 0$ and $\psi_2^2(\alpha) \neq 0$. Then we have that $\psi_2^2(F(X))$ has exactly three zeros which are the zeros of $\psi_2^2(X)$. If $d = 1$, putting $F(X) = aX + b$, we obtain that the polynomials $X^3 + AX + B$ and $a^3X^3 + 3a^2bX^2 + (3ab^2 + aA)X + b^3 + Ab + B$ have exactly the same three zeros. We then have $3a^2b = 0$ and $a \neq 0$. Thus $b = 0$, and if we suppose $A \neq 0$ and $B \neq 0$, we have $a = 1$ which is impossible since $F(X) \neq X$. If $d \geq 2$, for all $i \in \{1, 2, 3\}$, the equation $F(X) = \alpha_i$ has exactly one solution γ_i of multiplicity d which is one of $\{\alpha_1, \alpha_2, \alpha_3\}$. Then γ_1 and γ_2 are the zeros of the $(d-1)$-derivative of $F(X)$ which is of degree 1 and this is impossible because $\gamma_1 \neq \gamma_2$. Hence in all cases, we obtain a contradiction. So there exists $\alpha \in \overline{\mathbb{F}_p}$ such that: $\psi_2^2(F(\alpha)) = 0$ and $\psi_2^2(\alpha) \neq 0$.

Lemma 3 *Let $E : y^2 = x^3 + Ax + B$ be an elliptic curve over $\mathbb{F}_p$. Let $k = 2^i$ for $i > 0$ an integer. Let $F(X) \in \mathbb{F}_p[X]$ be a non-constant polynomial with $\deg(F) \geq 2$. Then there exists $\alpha \in \overline{\mathbb{F}_p}$ such that $\psi_k^2(F(\alpha)) = 0$ and $\psi_k^2(\alpha) \neq 0$.*

Proof The univariate polynomial $\psi_k^2(X)$ has at least $k^2/2$ distinct zeros because $p \nmid k$. For all α such that $\psi_k^2(\alpha) = 0$, there exists at least one $\beta \in \overline{\mathbb{F}_p}$ such that $F(\beta) = \alpha$ and two such roots β (corresponding to two different α) are different. Since $\deg(F) \geq 2$, it follows that the equation $F(X) = \alpha$, for α zero of $\psi_k^2(X)$ has at least two different solutions. Hence, the polynomial $\psi_k^2(F(X))$ has at least k^2 distinct zeros and the result follows.

We also need the following lemmas from [8] and [6] about the distribution of products $\mathbf{a}^x$ in $\mathbb{F}_\ell^*$.

Lemma 4 ([8]) *Let $m \geq 1$ be an integer. For any $\Delta > 0$ and for all but at most $2^{-m}\Delta^{-1}(\ell-1)^{m+2}$ vectors $\mathbf{a} = (a_1, \ldots, a_m) \in (\mathbb{F}_\ell^*)^m$, the products $\mathbf{a}^x$ for $x \in \{0,1\}^m$ take at least $\ell - 1 - \Delta$ values in $\mathbb{F}_\ell^*$.*

Lemma 5 ([6]) *Let $n \geq j > 0$ be two integers. For all but at most $(3^j - 1)(\ell-1)^{n-1}/2$ vectors $\mathbf{a} = (a_1, \ldots, a_n) \in (\mathbb{F}_\ell^*)^n$ the products $\mathbf{a}^x$ for $x \in \{0,1\}^n$ take at least 2^j values in $\mathbb{F}_\ell^*$.*

3 Polynomial Interpolation of the Naor-Reingold Pseudo-Random Function over Finite Fields

In this section, p is an odd prime number, n is an integer and $g \in \mathbb{F}_p^*$ is an element of prime order ℓ (with $\ell \mid p-1$). We prove results on the univariate and multivariate polynomial interpolation of the Naor-Reingold pseudo-random function over finite fields. We consider polynomials that interpolates values of the Naor-Reingold pseudo-random function for a fixed secret key $\mathbf{a} \in (\mathbb{F}_\ell^*)^n$. The values considered are evaluation of the function at integers $x \in \{0, \cdots, 2^n - 1\}$ and translates of these values by some fixed constants $t_1, t_2, \cdots, t_k \in \mathbb{N}$. This setting is interesting for applications in cryptography. Note that if one value $x + t_i$ is larger than 2^n for some $i \in \{1, \ldots, k\}$ then, the Naor-Reingold function is not defined at $x + t_i$. In the following, we consider simple sets where all translates belong to the Naor-Reingold function domain but our method can be adapted to other settings.

First, we consider multivariate polynomial interpolation over large sets of values.

Theorem 1 *Let $t \geq 1$ be an integer. Let $t_1, t_2, \cdots, t_k$ be fixed distinct integers such that $t_1, t_2, \cdots, t_k < 2^t$ and let $A \subseteq \{0, \cdots, 2^n - 1\}$. For some $\mathbf{a} \in (\mathbb{F}_\ell^*)^n$, let $F_{\mathbf{a}}(X_1, \ldots, X_k) \in \mathbb{F}_p[X_1, \cdots, X_k]$ such that*

$$F_{\mathbf{a}}(f_{\mathbf{a}}(x), f_{\mathbf{a}}(x+t_1), \cdots, f_{\mathbf{a}}(x+t_{k-1})) = f_{\mathbf{a}}(x+t_k) \tag{1}$$

for all $x \in A$. For all but at most $2k(\ell-1)^{n-1}$ vectors $\mathbf{a} \in (\mathbb{F}_\ell^*)^n$, we have

$$\begin{cases} \binom{\deg(F_{\mathbf{a}}) + k}{k} \geq \dfrac{\ell}{2\Delta + 1} - 1 \\ w(F_{\mathbf{a}}) \geq \dfrac{\ell}{2\Delta + 1} - 1 \end{cases}$$

where $\Delta = \ell - 1 - \sharp S$ for the set $S = \{\mathbf{a}^{2^t x} \in \mathbb{F}_\ell^* : 2^t x \in A\}$,

It is worth noting that the conclusion of Theorem 1 cannot hold for all vectors $\mathbf{a} \in (\mathbb{F}_\ell^*)^n$. For instance, if we consider a secret key $\mathbf{a} = (a_1, \ldots, a_n) \in (\mathbb{F}_\ell^*)^n$ such that $a_{n-1} = a_n$ and the simple case $k = 1$ and $t_1 = 1$, we have $f_{\mathbf{a}}(x + t_1) = f_{\mathbf{a}}(x)$ for all integer x in the set $A = \{x \in \{0, \cdots, 2^n - 1\}, x \equiv 1 \bmod 4\}$, (since $x = (x_1, x_2, \ldots, x_{n-2}, 0, 1)$ and $x + t_1 = (x_1, x_2, \ldots, x_{n-2}, 1, 0)$). The polynomial $F_{\mathbf{a}}(X_1) = X_1$ of degree 1 and weight 1 therefore satisfies (1) for all $x \in A$ where the set A is very large since $\sharp A = 2^{n/4}$. However, Theorem 1 ensures that the lower bounds on the degree and the weight of F hold with probability $1 - 2k/(\ell - 1)$ when the secret key $\mathbf{a}$ is picked uniformly at random (and hence with overwhelming probability for k polynomial in the security parameter).

In Theorem 1 statement, it is also necessary to consider the cardinality of a subset of $\{\mathbf{a}^x \in \mathbb{F}_\ell^*, x \in A\}$ and not the cardinality of A itself since it is possible that for some secret key $\mathbf{a}$, the latter is "large" while the former is "small". For instance, for a secret key $\mathbf{a} = (a, \ldots, a) \in (\mathbb{F}_\ell^*)^n$ (where all components are equal to some constant value $a \in \mathbb{F}_\ell^*$), we have $f_{\mathbf{a}}(x) = g^{\mathbf{a}^x} = g^{\mathbf{a}^{\mathrm{hw}(x)}}$ where $\mathrm{hw}(x)$ denotes x's Hamming weight (i.e., its number of non-zero coordinates). In this case, even if the set A is very large, $\{\mathbf{a}^x \in \mathbb{F}_\ell^*, x \in A\}$ is of cardinality at most n and one can construct a small degree multivariate polynomial that interpolates the values of the Naor-Reingold pseudo-random function.

Proof Since $t_1, t_2, \cdots, t_k < 2^t$, we have

$$\mathbf{a}^{2^t x + t_i} = \mathbf{a}^{2^t x} \mathbf{a}^{t_i}$$

for all $x \in A$ such that $2^t x \leq 2^n - 1$ and $i \in \{1, \cdots, k\}$. The relation (1) thus becomes

$$F_{\mathbf{a}}(g^u, g^{u\mathbf{a}^{t_1}}, \cdots, g^{u\mathbf{a}^{t_k - 1}}) = g^{u\mathbf{a}^{t_k}},$$

for all $u \in S$. Let $R = \{u \in S | u(\mathbf{a}^{t_k})^{-1} \in S\}$. We put $\Delta = \ell - 1 - \sharp S$ and, by the union bound, we have $\sharp R \geq \ell - 1 - 2\Delta$ and

$$F_{\mathbf{a}}(g^{u(\mathbf{a}^{t_k})^{-1}}, \cdots, g^{u\mathbf{a}^{t_k - 1}(\mathbf{a}^{t_k})^{-1}}) = g^u,$$

for all $u \in R$.

Let $H_{\mathbf{a}}(X) = F_{\mathbf{a}}(X^{(\mathbf{a}^{t_k})^{-1}}, \cdots, X^{\mathbf{a}^{t_k - 1}(\mathbf{a}^{t_k})^{-1}}) - X \in \mathbb{F}_p[X]$ and $K_{\mathbf{a}}(X)$ the polynomial obtained from $H_{\mathbf{a}}(X)$ by considering the degree of monomials of $H_{\mathbf{a}}(X)$ modulo ℓ.

Claim The polynomial $K_{\mathbf{a}}(X)$ is not a zero polynomial for all but at most $2k(\ell - 1)^{n-1}$ vectors $\mathbf{a} \in (\mathbb{F}_\ell^*)^n$.

Proof (Claim.) Indeed if $K_{\mathbf{a}}(X)$ is a zero polynomial, then

- either $F_{\mathbf{a}}$ is a monomial of the form $X_1^{\alpha_1} \cdots X_k^{\alpha_k}$, with $(\alpha_1, \cdots, \alpha_k) \neq (0, \cdots, 0)$

– or $F_{\mathbf{a}}$ would be a sum of at least two monomials $X_1^{\alpha_1}\cdots X_k^{\alpha_k}$ and $X_1^{\beta_1}\cdots X_k^{\beta_k}$ and there would exist $(\alpha_1,\cdots,\alpha_k)\neq(\beta_1,\cdots,\beta_k)$ such that

$$\alpha_1(\mathbf{a}^{t_k})^{-1}+\cdots+\alpha_k\mathbf{a}^{t_{k-1}}(\mathbf{a}^{t_k})^{-1}=\beta_1(\mathbf{a}^{t_k})^{-1}+\cdots+\beta_k\mathbf{a}^{t_{k-1}}(\mathbf{a}^{t_k})^{-1}$$

in $\mathbb{F}_\ell$.

If $F_{\mathbf{a}}$ is of the form $X_1^{\alpha_1}\cdots X_k^{\alpha_k}$, then from (1), it will follows that

$$\alpha_1\mathbf{a}^{x}+\cdots+\alpha_k\mathbf{a}^{x+t_{k-1}}=\mathbf{a}^{x+t_k}\quad\text{in }\mathbb{F}_\ell\text{, for all } x\in A. \tag{2}$$

Let x such that (2) is satisfied. Then we can easily prove for all $n\geq 1$ by induction in k that the number of $a\in(\mathbb{F}_\ell^*)^n$ solutions of (2) does not exceed $k(\ell-1)^{n-1}$.

1. For $k=0$, the equation $\mathbf{a}^{x+t_k}=0$ has no solution and the statement is clearly true.
2. Otherwise, let $j=\max(\{i\in\{1\ldots,k\}|\alpha_i\neq 0\})$. Because $x+t_k\neq x+t_j$, there exists i such that i-th component of $x+t_k$ is different from the i-th component of $x+t_j$. Then the above equation can be written in the form $T_1=T_2a_i$ where T_1 and T_2 do not depend on a_i. If $T_2\neq 0$, then for any vector $(a_1,\cdots,a_{i-1},a_{i+1},\cdots,a_n)\in(\mathbb{F}_\ell^*)^{n-1}$, the value of a_i is defined uniquely. If $T_2=0$, then by induction, the number of $(a_1,\cdots,a_{i-1},a_{i+1},\cdots,a_n)\in(\mathbb{F}_\ell^*)^{n-1}$ does not exceed $(k-1)(\ell-1)^{n-1}$. Therefore, the number of solutions does not exceed $(k-1)(\ell-1)^{n-1}+(\ell-1)^{n-1}=k(\ell-1)^{n-1}$, and the result follows.

   In the second case, if there exists $(\alpha_1,\cdots,\alpha_k)\neq(\beta_1,\cdots,\beta_k)$ such that

$$\alpha_1(\mathbf{a}^{t_k})^{-1}+\cdots+\alpha_k\mathbf{a}^{t_{k-1}}(\mathbf{a}^{t_k})^{-1}=\beta_1(\mathbf{a}^{t_k})^{-1}+\cdots+\beta_k\mathbf{a}^{t_{k-1}(\mathbf{a}^{t_k})^{-1}}$$

in $\mathbb{F}_\ell$ then we have

$$(\alpha_1-\beta_1)\mathbf{a}^0+\cdots+(\alpha_k-\beta_k)\mathbf{a}^{t_{k-1}}=0$$

in $\mathbb{F}_\ell$. Then by proceeding as previously by induction on k, for all n, one can see that the number of solutions $a\in(\mathbb{F}_\ell^*)^n$ does not exceed $(k-1)(\ell-1)^{n-1}$.

For $\mathbf{a}\in(\mathbb{F}_\ell^*)^n$ such that $K_{\mathbf{a}}(X)$ is not a zero polynomial, we have by Lemma 1, that $w(K_{\mathbf{a}}(X))\geq\frac{\ell}{\ell-(\ell-1-2\Delta)}$, since $\deg(K_{\mathbf{a}}(X))\leq\ell-1$ and $K_{\mathbf{a}}(X)$ has at least $\ell-1-2\Delta$ roots of the g^u. Therefore, by Lemma 1, we have

$$\begin{cases}\binom{\deg(F_{\mathbf{a}})+k}{k}\geq\dfrac{\ell}{2\Delta+1}\\ w(F_{\mathbf{a}})\geq\dfrac{\ell}{2\Delta+1}-1\end{cases}$$

for all but at most $2k(\ell-1)^{n-1}$ vectors $\mathbf{a}\in(\mathbb{F}_\ell^*)^n$ and the result follows.

Remark 1 Theorem 1 is non-trivial only when $\sharp S\geq(3\ell-2)/4$. Since $\sharp S\leq 2^{n-t}$, Theorem 1 only applies to settings where the message length n is greater than the sum of the bit-length of the underlying group order and t.

The cardinality of the set S depends on A and on the secret key $\mathbf{a} = (a_1, \ldots, a_n) \in (\mathbb{F}_\ell^*)^n$. In the following lemma for certain condition on A and on n, we show that $\sharp S$ is close to ℓ for almost all secret key $\mathbf{a}$. This allows us to obtain Corollary 1 and for the forthcoming theorems in this paper to obtain non trivial lower bounds.

Lemma 6 *Let $\gamma > \delta > 0$ such that $n \geq (1+\gamma)\log(\ell-1)$.*
Let $t = \lfloor \min(1, (\gamma-\delta)/2)\log(\ell-1) \rfloor - 1$ and let $A \subseteq \{0, \cdots, 2^n-1\}$ such that $\{2^t x : x \in \{0, \ldots, 2^{n-t}-1\}\} \subseteq A$. Putting $\Gamma = \lfloor (\ell-1)2^{-t} \rfloor$, we obtain:

$$\sharp S \geq \ell - 1 - \Gamma,$$

for all but at most $(\ell-1)^{n-\delta}$ vectors $\mathbf{a} \in (\mathbb{F}_\ell^*)^n$.

Proof We denote again $S = \{\mathbf{a}^{2^t x} \in \mathbb{F}_\ell^* : 2^t x \in A\}$.

Putting $\Gamma = \lfloor (\ell-1)2^{-t} \rfloor$ and applying Lemma 4, we have $\sharp S \geq \ell - 1 - \Gamma$ for all but at most $2^{t-n}\Gamma^{-1}(\ell-1)^{n+2} \leq (\ell-1)^{n-\delta}$ vectors $\mathbf{a} \in (\mathbb{F}_\ell^*)^n$.

We apply Lemma 6 to Theorem 1 to obtain the following corollary:

Corollary 1 *Let $\gamma > \delta > 0$ such that $n \geq (1+\gamma)\log(\ell-1)$. Let $t = \lfloor \min(1, (\gamma-\delta)/2)\log(\ell-1) \rfloor - 1$ and $t_1, t_2, \cdots, t_k$ be fixed distinct integers such that $t_1, t_2, \cdots, t_k < 2^t$ and let $A \subseteq \{0, \cdots, 2^n-1\}$. For some $a \in (\mathbb{F}_\ell^*)^n$, let $F_{\mathbf{a}}(X_1, \ldots, X_k) \in \mathbb{F}_p[X_1, \cdots, X_k]$ such that Relation (1) holds for all $x \in A$. If $\{2^t x : x = 0, \ldots, 2^{n-t}-1\} \subseteq A$, we have*

$$\begin{cases} \binom{\deg(F_{\mathbf{a}}) + k}{k} \geq \frac{1}{8}(\ell-1)^{\min(1,(\gamma-\delta)/2)} \\ w(F_{\mathbf{a}}) \geq \frac{1}{8}(\ell-1)^{\min(1,(\gamma-\delta)/2)} - 1 \end{cases}$$

for all but at most $2k(\ell-1)^{n-1} + (\ell-1)^{n-\delta}$ vectors $\mathbf{a} \in (\mathbb{F}_\ell^*)^n$.

The proof is straightforward since, with the previous notation, we have in this case $\Delta < \Gamma$. Likewise Lemma 6 can be applied to the next theorems of this paper to obtain non-trivial lower bounds for almost all vectors $\mathbf{a} \in (\mathbb{F}_\ell^*)^n$.

For the cases where the cardinality of the set S is smaller than $(3\ell-2)/4$, Theorem 1 does not give a non-trivial lower bound on F's degree. In the next theorem, we obtain such a lower bound for much smaller sets S with $\#S \in [\sqrt{\ell}+1, (3\ell-2)/4]$. Theorem 2 only applies for univariate interpolation (i.e. $k = 1$).

Theorem 2 *Let $t \geq 1$ be a fixed integer and let $A \subseteq \{0, \cdots, 2^n-1\}$. For some $\mathbf{a} \in (\mathbb{F}_\ell^*)^n$, let $F_{\mathbf{a}}(X) \in \mathbb{F}_p[X]$ such that*

$$F_{\mathbf{a}}(f_{\mathbf{a}}(x)) = f_{\mathbf{a}}(x+t) \tag{3}$$

for all $x \in A$. For all but at most $2(\ell-1)^{n-1}$ vectors $\mathbf{a} \in (\mathbb{F}_\ell^*)^n$, we have

$$\deg(F_{\mathbf{a}}) \geq \frac{\sharp S(\sharp S - 1)}{\ell - 1}.$$

where $S = \{\mathbf{a}^{2^t x} \in \mathbb{F}_\ell^* : 2^t x \in A\}$.

Proof As in the previous proof, we have

$$F_{\mathbf{a}}(g^u) = g^{u\mathbf{a}^t} \quad \text{for all } u \in S.$$

Consider

$$D = \{1 \leq b \leq \ell - 1 : b \equiv y - x \mod \ell,\ x, y \in S\}.$$

There exists $b \in D$ such that there are at least

$$\frac{\sharp S(\sharp S - 1)}{\sharp D} \geq \frac{\sharp S(\sharp S - 1)}{\ell - 1}$$

representations $b \equiv y - x \bmod \ell$, with $x, y \in S$. We choose this b and put

$$R = \{x \in S : b + x \equiv y \bmod \ell,\ y \in S\}.$$

Then we have

$$\sharp R \geq \frac{\sharp S(\sharp S - 1)}{\ell - 1}.$$

For $u \in R$, (since $g^x = g^{x+\ell}$, for all x), we have

$$\begin{aligned} F_{\mathbf{a}}(g^{u+b}) &= g^{(u+b)\mathbf{a}^t} \\ &= g^{u\mathbf{a}^t} \times g^{b\mathbf{a}^t} \\ &= F_{\mathbf{a}}(g^u) \times g^{b\mathbf{a}^t} \end{aligned}$$

Let $H_{\mathbf{a}}(X) = F_{\mathbf{a}}(g^b X) - g^{b\mathbf{a}^t} F_{\mathbf{a}}(X)$. Then $H_{\mathbf{a}}(X)$ has at least $\sharp R$ zeros. As in the previous proof, $H_{\mathbf{a}}(X) \neq 0$ for all but at most $2(\ell-1)^{n-1}$ vectors $\mathbf{a} \in (\mathbb{F}_\ell^*)^n$ and $\deg(H_{\mathbf{a}}) \leq \deg(F_{\mathbf{a}})$, we have

$$\deg(F_{\mathbf{a}}) \geq \frac{\sharp S(\sharp S - 1)}{\ell - 1}.$$

for all but at most $2(\ell - 1)^{n-1}$ vectors $a \in (\mathbb{F}_\ell^*)^n$.

In the following lemma, we show that that there exists numerous sets A and corresponding S such that $\#S \in [\sqrt{\ell} + 1, (3\ell - 2)/4]$. For such sets Theorem 1 does not give a non-trivial lower bound on F's degree.

Lemma 7 *Let* $\frac{1}{\log(3)} - \frac{1}{2} > \delta > 0$ *(with* $\frac{1}{\log(3)} - \frac{1}{2} \simeq 0.1309\ldots$*).*
Let $t \geq 1$ *and* n *be integers such that* $n = t + \lceil (1/2 + \delta)\log(\ell - 1) \rceil + s$ *for some integer* s *such that* $0 \leq s \leq \log(3\ell - 2) - 2 - \lceil (1/2 + \delta)\log(\ell - 1) \rceil$. *Let* $A \subseteq \{0, \cdots, 2^n - 1\}$ *such that* $\{2^t x : x \in \{0, \ldots, 2^{n-t} - 1\}\} \subseteq A$. *Putting* $\gamma = 1 - \log(3)(1/2 + \delta)$ *we obtain:*

$$(3\ell - 2)/4 \geq \sharp S \geq (\ell - 1)^{(1/2+\delta)}$$

for all but at most $3/2(\ell - 1)^{n-\gamma}$ *vectors* $\mathbf{a} \in (\mathbb{F}_\ell^*)^n$.

Proof We denote again $S = \{\mathbf{a}^{2^t x} \in \mathbb{F}_\ell^* : 2^t x \in A\}$.
Putting $j = \lceil (1/2+\delta)\log(\ell-1)\rceil$ and applying Lemma 5, we obtain readily $\sharp S \geq (\ell-1)^{(1/2+\delta)}$ for all but at most $(3^j-1)(\ell-1)^{n-1} \leq 3/2(\ell-1)^{n-\gamma}$ vectors $\mathbf{a} \in (\mathbb{F}_\ell^*)^n$. Since $\sharp S \leq 2^{j+s} \leq (3\ell-2)/4$, we obtain the desired result.

For such sets A and S and parameters n, t, s given in Lemma 7, we have (using the notation of Theorem 2), that the degree of of polynomial $F_\mathbf{a}$ satisfying (3) verifies $\deg(F_\mathbf{a}) \geq c \cdot \ell^{2\delta}$ for all but at most $2(\ell-1)^{n-1} + 3/2(\ell-1)^{n-\gamma}$ vectors $\mathbf{a} \in (\mathbb{F}_\ell^*)^n$ (where c is an absolute constant close to 1).

Remark 2 This proof technique cannot be used to obtain a lower bound on the weight of a univariate polynomial F or on the degree of a multivariate polynomial F for $k \geq 2$ and it remains an open problem to improve Theorem 1 for smaller sets S with $\#S \leq (3\ell-2)/4$ in these settings.

4 Univariate Interpolation of the Naor-Reingold Pseudo-Random Function over Elliptic Curves

In this section, p is an odd prime number, n is an integer, E is an elliptic curve over $\mathbb{F}_p$ and P is a point of the curve E with prime order ℓ (with $\ell \mid \#E(\mathbb{F}_p)$). We prove results on the univariate polynomial interpolation of the Naor-Reingold pseudo-random function from elliptic curves defined by $f_\mathbf{a}(x) = X([\mathbf{a}^x]P)$ for a secret key $\mathbf{a} \in (\mathbb{F}_\ell^*)^n$ and an integer $x \in \{0, 1, \ldots, 2^n - 1\}$ (where $X(Q)$ denotes the abscissa of a point $Q \in E(\mathbb{F}_p)$). First, we consider interpolation over large sets of values.

Theorem 3 *Let $E : y^2 = x^3 + \gamma x + \delta$ be an elliptic curve over $\mathbb{F}_p$ with $\gamma\delta \neq 0$. Let $t \geq 1$ be a fixed integer and let $A \subseteq \{0, \cdots, 2^n - 1\}$. For some $\mathbf{a} \in (\mathbb{F}_\ell^*)^n$, let $F_\mathbf{a}(X) \in \mathbb{F}_p[X]$ such that*

$$F_\mathbf{a}(f_\mathbf{a}(x)) = f_\mathbf{a}(x+t) \tag{4}$$

for all $x \in A$. For all but at most $2(\ell-1)^{n-1}$ vectors $\mathbf{a} \in (\mathbb{F}_\ell^*)^n$, we have

$$\deg(F_\mathbf{a}) \geq \frac{2\sharp S - (\ell-1)}{14}.$$

where $S = \{\mathbf{a}^{2^t x} \in \mathbb{F}_\ell^* : 2^t x \in A\}$.

Proof We have $F_\mathbf{a}(x_u) = x_{u\mathbf{a}^t}$ for all $u \in S$, where $x_t = X([t]P)$, for all $t \in \mathbb{F}_\ell$. We consider the $R = \{u \in S : 2u \in S\}$ with $\sharp R \geq \ell - 1 - 2\Delta$. For all $u \in R$, $2u \in S$ and $[2u]P \neq O$ and $F_\mathbf{a}(x_{2u}) = x_{2u\mathbf{a}^t}$ is well-defined in $\mathbb{F}_p$ and $x_{u\mathbf{a}^t}$ is thus not a root of ψ_2. Therefore, we have:

$$\begin{aligned} F_\mathbf{a}(x_{2u}) &= x_{2u\mathbf{a}^t} \\ &= \theta_2(x_{u\mathbf{a}^t})/\psi_2^2(x_{u\mathbf{a}^t}) \\ &= \theta_2(F_\mathbf{a}(x_u))/\psi_2^2(F_\mathbf{a}(x_u)), \quad \text{for all } u \in R. \end{aligned}$$

We thus get

$$F_{\mathbf{a}}\left(\frac{\theta_2(x_u)}{\psi_2^2(x_u)}\right) = \frac{\theta_2(F_{\mathbf{a}}(x_u))}{\psi_2^2(F_{\mathbf{a}}(x_u))}$$

for all $u \in R$. Finally, we consider the polynomial:

$$H_{\mathbf{a}}(X) = \psi_2^{2d}(X)\psi_2^2(F_{\mathbf{a}}(X))\left(F_{\mathbf{a}}\left(\frac{\theta_2(X)}{\psi_2^2(X)}\right) - \frac{\theta_2(F_{\mathbf{a}}(X))}{\psi_2^2(F_{\mathbf{a}}(X))}\right),$$

where $d = \deg(F_{\mathbf{a}})$. The polynomial $H_{\mathbf{a}}(X)$ has at least $\sharp R/2$ zeros. If $\mathbf{a}^t \neq \pm 1$, we will have $F_{\mathbf{a}}(X) \neq X$ and by Lemma 2, it will imply that there exists $\alpha \in \overline{\mathbb{F}_p}$ such that $\psi_2^2(F_{\mathbf{a}}(\alpha)) = 0$ and $\psi_2^2(\alpha) \neq 0$. Hence, we have $H_{\mathbf{a}}(\alpha) = -\theta_2(F_{\mathbf{a}}(\alpha))\psi_2^{2d}(\alpha) \neq 0$, since $\theta_2(X)$ and $\psi_2^2(X)$ have no common zeros.

Therefore, $H_{\mathbf{a}}(X)$ is a non-zero polynomial and $\deg(H_{\mathbf{a}}) \leq 7d$. Then we get that $7d \geq \sharp R/2$ and then $d \geq \frac{\ell-1-2\Delta}{14}$. Since $\mathbf{a}^t \neq \pm 1$ for all but at most $2(\ell-1)^{n-1}$ vectors $a \in (\mathbb{F}_\ell^*)^n$, the result follows.

Theorem 3 is only non-trivial if $\sharp S \geq (\ell+13)/2$. Again, the cardinality of the set S depends on A and on the secret key $\mathbf{a} = (a_1, \ldots, a_n) \in (\mathbb{F}_\ell^*)^n$, but using again Lemma 6, we can easily obtain (as in Corollary 1) non-trivial lower bounds for specific sets A and parameter n.

In the following theorem, we obtain a lower bound for smaller sets S.

Theorem 4 *Let $t \geq 1$ be a fixed integer, $A \subseteq \{0, \cdots, 2^n - 1\}$, $0 < \epsilon < 1$ and $S = \{\mathbf{a}^{2^t x} \in \mathbb{F}_\ell^* : 2^t x \in A\}$ with $\sharp S \geq \frac{2(\ell-1)}{\epsilon \log(\ell)}$. For some $\mathbf{a} \in (\mathbb{F}_\ell^*)^n$, let $F_{\mathbf{a}}(X) \in \mathbb{F}_p[X]$ such that*

$$F_{\mathbf{a}}(f_{\mathbf{a}}(x)) = f_{\mathbf{a}}(x+t) \tag{5}$$

for all $x \in A$. For all but at most $2(\ell-1)^{n-1}$ vectors $\mathbf{a} \in (\mathbb{F}_\ell^*)^n$, we have

$$\deg(F_{\mathbf{a}}) \geq \frac{\sharp S}{4\epsilon \log(\ell) \times \ell^{2\epsilon}}.$$

Proof We have $F_{\mathbf{a}}(x_u) = x_{u\mathbf{a}^t}$ for all $u \in S$ where, as above, we denote $x_t = X([t]P)$, for all $t \in \mathbb{F}_\ell$. Let K be an integer and let us consider the sets

$$S_i = \{1 \leq b \leq \ell - 1 : 2^i m \equiv b \bmod \ell,\ m \in S\},$$

for $0 \leq i \leq K$, and $R_{i,j} = S_i \cap S_j$ for $0 \leq i < j \leq K$. We have

$$(K+1)\sharp S - \sum_{0 \leq i < j \leq K} \sharp R_{i,j} \leq \sharp\left(\bigcup_{i=0}^{K} S_i\right) \leq \ell - 1.$$

Therefore, there is a pair $0 \leq i < j \leq K$ such that

$$\sharp R_{0,j-i} = \sharp R_{i,j} \geq \frac{2((K+1)\sharp S - (\ell-1))}{K(K+1)}.$$

For $u \in R_{0,j-i}$, there exists a unique $m \in S$ such that $2^{j-i}m \equiv u \bmod \ell$, with $u \in S$ and the corresponding m's are distinct for two different u's. Since

$x_k = x_{k+l}$ for all k, then we have $F_{\mathbf{a}}(x_{2^{j-i}m}) = x_{2^{j-i}m\mathbf{a}^t}$ for at least $\sharp R_{0,j-i}$ different $m \in S$. For each such m, we have

$$\begin{aligned} F_{\mathbf{a}}\left(\frac{\theta_{2^{j-i}}(x_m)}{\psi^2_{2^{j-i}}(x_m)}\right) &= x_{2^{j-i}m\mathbf{a}^t} \\ &= \theta_{2^{j-i}}(x_{m\mathbf{a}^t})/\psi^2_{2^{j-i}}(x_{m\mathbf{a}^t}) \\ &= \theta_{2^{j-i}}(F_{\mathbf{a}}(x_m))/\psi^2_{2^{j-i}}(F_{\mathbf{a}}(x_m)), \end{aligned}$$

since $m \in S$. Finally, we consider the polynomial

$$H_{\mathbf{a}}(X) = \psi^{2d}_{2^{j-i}}(X)\psi^2_{2^{j-i}}(F_{\mathbf{a}}(X))\left(F_{\mathbf{a}}\left(\frac{\theta_{2^{j-i}}(X)}{\psi^2_{2^{j-i}}(X)}\right) - \frac{\theta_{2^{j-i}}(F_{\mathbf{a}}(X))}{\psi^2_{2^{j-i}}(F_{\mathbf{a}}(X))}\right),$$

where $d = \deg(F_{\mathbf{a}})$.

The polynomial $H_{\mathbf{a}}(X)$ has at least $\sharp R_{0,j-i}$ zeros. Since $d \geq 2$ and 2^{j-i} and p are coprime, then by Lemma 3, there exists $\alpha \in \overline{\mathbb{F}_p}$ such that $\psi^2_{2^{j-i}}(F_{\mathbf{a}}(\alpha)) = 0$ and $\psi^2_{2^{j-i}}(\alpha) \neq 0$. Hence, we have $H_{\mathbf{a}}(\alpha) = -\theta_{2^{j-i}}(F_{\mathbf{a}}(\alpha))\psi^{2d}_{2^{j-i}}(\alpha) \neq 0$, since $\theta_{2^{j-i}}(X)$ and $\psi^2_{2^{j-i}}(X)$ have no common zeros.

Therefore $H_{\mathbf{a}}(X)$ is a non-zero polynomial and $\deg(H_{\mathbf{a}}) \leq d(2(2^{j-i})^2 - 1)$ and we get

$$d \geq \frac{\sharp R_{0,j-i}}{2(2^{2(j-i)+1} - 1)} \geq \frac{(K+1)\sharp S - (\ell - 1)}{K(K+1)(2^{2(j-i)+1} - 1)}.$$

Since $j - i \leq K$, then we have

$$\begin{aligned} d \geq \frac{(K+1)\sharp S - (\ell-1)}{K(K+1)(2^{2K+1}-1)} &\geq \frac{1}{2^{2K+1}-1}\left(\frac{\sharp S}{K} - \frac{\ell - 1}{K(K+1)}\right) \\ &\geq \frac{\sharp S}{K(2^{2K+1}-1)}\left(1 - \frac{\ell - 1}{\sharp S(K+1)}\right). \end{aligned}$$

Letting $K = \lfloor \epsilon \log(\ell) \rfloor$, for any $0 < \epsilon < 1$, we have

$$d \geq \frac{\sharp S}{2\epsilon \log(\ell) \times \ell^{2\epsilon}}\left(1 - \frac{\ell - 1}{\sharp S \epsilon \log(\ell)}\right) \geq \frac{\sharp S}{4\epsilon \log(\ell) \times \ell^{2\epsilon}}.$$

Theorem 4 also applies to numerous sets A and S for which Theorem 3 does not apply. For instance, we can consider parameters n, t, s given in Lemma 7 such that $2^{n-t-s} \geq \frac{2(\ell-1)}{\epsilon \log(\ell)}$.

5 Bivariate Interpolation of the Naor-Reingold Pseudo-Random Function over Elliptic Curves

It seems rather difficult to obtain an analogue of Theorem 1 in the case of elliptic curves. In this section, we use the methods from [13] and we prove results on bivariate interpolation of the Naor-Reingold pseudo-random function from elliptic curves (but in a slightly different setting). We use the notation from the previous section and, as before, we consider first interpolation over large sets of values.

Theorem 5 *Let $A_1, A_2 \subseteq \{0, \cdots, 2^n - 1\}$ and $t \geq 1$ be an integer. For some $\mathbf{a} \in (\mathbb{F}_\ell^*)^n$, let $F_{\mathbf{a}}(X, Y) \in \mathbb{F}_p[X, Y]$ such that*

$$F_{\mathbf{a}}(f_{\mathbf{a}}(x), f_{\mathbf{a}}(x')) = f_{\mathbf{a}}(x + x') \tag{6}$$

for all $(x, x') \in A_1 \times A_2$. We have

$$\deg(F_{\mathbf{a}}) \geq \min\left(\lfloor(\ell - 1)/\Delta\rfloor - 2; \lceil(\sharp S_2 - 1)^{1/3}\rceil - 2\right).$$

where $\Delta = \ell - 1 - \sharp S_1$ for the set $S_1 = \{\mathbf{a}^x : x \in A_1\,, x < 2^t\}$ and where $S_2 = \{\mathbf{a}^{2^t x'} \in \mathbb{F}_\ell^* : 2^t x' \in A_2\}$.

Proof We may suppose $\sharp S_2 \geq 10$ since otherwise the result is trivial. We denote

$$d = \min\left(\lfloor(\ell - 1)/\Delta\rfloor - 2; \lceil(\sharp S_2 - 1)^{1/3}\rceil - 2\right).$$

We have

$$F_{\mathbf{a}}(x_u, x_{u'}) = x_{uu'}, \quad \text{for all } u \in S_1 \text{ and } u' \in S_2.$$

Let R be the set of $u \in S_1$ such that

$$ia \bmod \ell \in S_1, \quad \forall i \in \{1, \cdots, d + 1\}.$$

The cardinality of R is at least $\ell - 1 - \Delta(d + 1)$. Let $u \in R$, then we have

$$F_{\mathbf{a}}(x_{(i+1)u}, x_{v_j}) = x_{(i+1)uv_j}, \quad \text{for all } 0 \leq i, j \leq d,$$

where $v_0, \cdots, v_d$ are any distinct elements of S_2.

Let us suppose that $\deg_X(F_{\mathbf{a}}), \deg_Y(F_{\mathbf{a}}) \leq d$ namely

$$F_{\mathbf{a}}(X, Y) = \sum_{i,j=0}^{d} c_{i,j} X^i Y^j,$$

then we have for $0 \leq k, \ell \leq d$,

$$x_{(k+1)uv_\ell} = \sum_{i,j=0}^{d} c_{i,j} x_{(k+1)u}^i x_{v_\ell}^j.$$

Then $F_{\mathbf{a}}$'s coefficients are determined by the following matrix equation:

$$\begin{aligned} C &= \begin{pmatrix} c_{0,0} & \cdots & c_{0,d} \\ \vdots & & \vdots \\ c_{d,0} & \cdots & c_{d,d} \end{pmatrix} \\ &= \begin{pmatrix} x_u^0 & \cdots & x_u^d \\ \vdots & & \vdots \\ x_{(d+1)u}^0 & \cdots & x_{(d+1)u}^d \end{pmatrix}^{-1} \begin{pmatrix} x_{uv_0} & \cdots & x_{uv_d} \\ \vdots & & \vdots \\ x_{(d+1)uv_0} & \cdots & x_{(d+1)uv_d} \end{pmatrix} \begin{pmatrix} x_{v_0}^0 & \cdots & x_{v_d}^0 \\ \vdots & & \vdots \\ x_{v_0}^d & \cdots & x_{v_d}^d \end{pmatrix} \end{aligned}$$

The matrix C is non-singular if and only if the middle matrix on the right hand is non-singular. A subset $\{v_0, \cdots, v_d\}$ of S_2 with this property exists if

and only if the vectors $T_k = (x_{kub})_{b\in S_2}$ for $k \in \{1,\cdots,d+1\}$ are linearly independent. If these vectors were linearly dependent, then there would exist an integer ω with $1 \le \omega \le d+1$ and coefficients $d_1,\cdots,d_\omega \in \mathbb{F}_p$, $d_\omega \neq 0$, such that

$$\sum_{k=1}^{\omega} d_k x_{kub} = 0, \qquad b \in S_2.$$

As at most two points with first coordinate equal to 0 exist on the elliptic curve and $\sharp S_2 \ge 3$, we get $\omega \ge 2$. Since $x_{kub} = \theta_k(x_{ub})/\psi_k^2(x_{ub})$, the polynomial

$$H(X) = \sum_{k=1}^{\omega} d_k \theta_k(X) \prod_{j=1, j\neq k}^{\omega} \psi_j^2(X)$$

has at least $\lfloor \sharp S_2/2 \rfloor$ zeros and degree at most

$$1 + \sum_{k=1}^{\omega}(k^2-1) = (2\omega^3 + 3\omega^2 - 5\omega + 6)/6 \le \omega^3/2 \le (d+1)^3/2.$$

Since $p \nmid \omega$, then points of order ω on E exist over $\overline{\mathbb{F}_p}$. Let $\alpha \in \overline{\mathbb{F}_p}$ be the first coordinate of a point of order ω. Then we have $\psi_\omega^2(\alpha) = 0$ and $H(\alpha) = d_\omega \theta_\omega(\alpha) \prod_{j=1}^{\omega-1} \psi_j^2(\alpha) \neq 0$.

The polynomial $H(X)$ is a non-zero polynomial and we have $(d+1)^3/2 \ge \lfloor \sharp S_2/2 \rfloor$ in contradiction with the definition of d. This shows that C is not singular and in particular each row of C has at least one non-zero entry and we have $\deg(F_{\mathbf{a}}) \ge \deg_X(F_{\mathbf{a}}) \ge d$.

Theorem 5 is non-trivial only for $\sharp S_1 \ge (\ell-1)/2$ and we can obtain (as in Corollary 1) non-trivial lower bounds on the degree of the interpolating polynomial for specific sets A_1 and A_2 and parameter t.

Lemma 8 *Let $m \ge 1$ be an integer, $\delta > 0$ and t be an integer such that $t \ge (1+\delta)\log(\ell-1) + m + 1$ and $n - t \ge (1+\delta)\log(\ell-1) + 2$.*
Let $A_1, A_2 \subseteq \{0,\cdots,2^n-1\}$ be two sets such that $\{0,\ldots,2^t-1\} \subseteq A_1$ and $\{2^t x' : x' \in \{0,\ldots,2^{n-t}-1\}\} \subseteq A_2$. Let $S_1 = \{\mathbf{a}^x : x \in A_1, x < 2^t\}$ and $S_2 = \{\mathbf{a}^{2^t x'} \in \mathbb{F}_\ell^* : 2^t x' \in A_2\}$, we have

$$\sharp S_1 \ge \ell - 1 - \lfloor (\ell-1)2^{-m} \rfloor \quad \text{and} \quad \sharp S_2 \ge (\ell-1)/2 + 1,$$

for all but at most $2(\ell-1)^{n-\delta}$ vectors $\mathbf{a} \in (\mathbb{F}_\ell^*)^n$.

Proof Let $\Delta = \lfloor (\ell-1)2^{-m} \rfloor$. Applying Lemma 4, we have $\sharp S_1 \ge \ell - 1 - \Delta$ for all but at most $2^{-t}\Delta^{-1}(\ell-1)^{t+2}(\ell-1)^{n-t} \le (\ell-1)^{n-\delta}$ vectors $\mathbf{a} \in (\mathbb{F}_\ell^*)^n$.

Likewise, applying Lemma 4 with $\Delta' = (\ell-1)/2 - 1$, we have $\sharp S_2 \ge (\ell-1)/2 + 1$ for all but at most $2^{t-n}\Delta'^{-1}(\ell-1)^{n-t+2}(\ell-1)^t \le (\ell-1)^{n-\delta}$ vectors $\mathbf{a} \in (\mathbb{F}_\ell^*)^n$.

We apply Lemma 8 to Theorem 5 to obtain the following corollary:

Corollary 2 *Let $m \geq 1$ be an integer and $\delta > 0$ such that $t \geq (1+\delta)\log(\ell-1)+m+1$ and $n-t \geq (1+\delta)\log(\ell-1)+2$.*
Let $A_1 \subseteq \{0,\cdots,2^n-1\}$ such that $\{0,\ldots,2^t-1\} \subseteq A_1$ and $A_2 \subseteq \{0,\cdots,2^n-1\}$ such that $\{2^t x' : x' \in \{0,\ldots,2^{n-t}-1\}\} \subseteq A_2$. For some $\mathbf{a} \in (\mathbb{F}_\ell^*)^n$, let $F_{\mathbf{a}}(X,Y) \in \mathbb{F}_p[X,Y]$ such that

$$F_{\mathbf{a}}(f_{\mathbf{a}}(x), f_{\mathbf{a}}(x')) = f_{\mathbf{a}}(x+x') \tag{7}$$

for all $(x,x') \in A_1 \times A_2$. We have

$$\deg(F_{\mathbf{a}}) \geq \min\left(2^m-2;\, ((\ell-1)/2)^{1/3}-2\right),$$

for all but at most $2(\ell-1)^{n-\delta}$ vectors $\mathbf{a} \in (\mathbb{F}_\ell^*)^n$.

The proof is straightforward since, with the of notation of Theorem 5, we have in this case $\Delta \leq (\ell-1)2^{-m}$ and $\sharp S_2 - 1 \geq (\ell-1)/2$.

To conclude the paper, we obtain a simple result for smaller sets S_1.

Theorem 6 *Let $A_1, A_2 \subseteq \{0,\cdots,2^n-1\}$ and $t \geq 1$ be an integer. For some $\mathbf{a} \in (\mathbb{F}_\ell^*)^n$, let $F_{\mathbf{a}}(X,Y) \in \mathbb{F}_p[X,Y]$ such that*

$$F_{\mathbf{a}}(f_{\mathbf{a}}(x), f_{\mathbf{a}}(x')) = f_{\mathbf{a}}(x+x') \tag{8}$$

for all $(x,x') \in A_1 \times A_2$. We have

$$\deg(F_{\mathbf{a}}) \geq \frac{\sharp S_1}{8}.$$

where $S_1 = \{\mathbf{a}^x : x \in A_1\,,\, x < 2^t\}$ and $S_2 = \{\mathbf{a}^{2^t x'} \in \mathbb{F}_\ell^* : 2^t x' \in A_2\}$ if there exists $v \in S_2$ such that $2v \in S_2$.

Proof We have

$$F_{\mathbf{a}}(x_u, x_v) = x_{uv} \quad \textit{and} \quad F_{\mathbf{a}}(x_u, x_{2v}) = x_{2uv} \quad \text{for all } u \in S_1.$$

Hence

$$F_{\mathbf{a}}\left(x_u, \frac{\theta_2(x_v)}{\psi_2^2(x_v)}\right) = \frac{\theta_2(x_{uv})}{\psi_2^2(x_{uv})} = \frac{\theta_2(F_{\mathbf{a}}(x_u,x_v))}{\psi_2^2(F_{\mathbf{a}}(x_u,x_v))} \quad \text{for all } u \in S_1.$$

Finally, we consider the polynomial

$$U(X) = \psi_2^2(F_{\mathbf{a}}(X,x_v))\left(F_{\mathbf{a}}(X, \frac{\theta_2(x_v)}{\psi_2^2(x_v)}) - \frac{\theta_2(F_{\mathbf{a}}(X,x_v))}{\psi_2^2(F_{\mathbf{a}}(X,x_v))}\right).$$

We have $\deg(U) \leq 4\deg(F_{\mathbf{a}})$. Let γ be a root of $\psi_2^2(X)$ and β such that $F_{\mathbf{a}}(\beta, x_v) = \gamma$. Then

$$U(\beta) = -\theta_2(F_{\mathbf{a}}(\beta,x_v)) \neq 0,$$

and U is non-zero polynomial. Since U has at least $\sharp S_1/2$ zeros, it follows that $4\deg(F_{\mathbf{a}}) \geq \sharp S_1/2$ i.e. $\deg(F_{\mathbf{a}}) \geq \frac{\sharp S_1}{8}$.

The condition on S_2 in the statement of Theorem 6 is achieved trivially when $\sharp S_2 > \frac{\ell-1}{2}$. It is worth mentioning that Theorem 6 also applies to many other sets. In the following lemma, we show that that there exists numerous sets A_1, A_2 and corresponding S_1, S_2 such that $\sharp S_1 \in [\sqrt{\ell}+1, (\ell-1)/2]$ and $\sharp S_2 > (\ell-1)/2$. For such sets Theorem 6 gives a non-trivial lower bound on the degree of the interpolating polynomial while Theorem 5 does not give a non-trivial lower bound on it. We apply Lemmas 4 and 5 like in the proof of Lemmas 6, 7 and 8 to obtain the following lemma:

Lemma 9 *Let* $\frac{1}{\log(3)} - \frac{1}{2} > \delta_1 > 0$ *(with* $\frac{1}{\log(3)} - \frac{1}{2} \simeq 0.1309\ldots$*) and* $\delta_2 > 0$. *Let* t *and* n *be integers such that* $t = \lceil (1/2+\delta_1)\log(\ell-1)\rceil + s$ *for some integer* s *such that* $0 \leq s \leq \log(\ell-1) - 1 - \lceil (1/2+\delta_1)\log(\ell-1)\rceil$ *and* $n - t \geq (1+\delta_2)\log(\ell-1)+2$. *Let* $A_1 \subseteq \{0,\cdots,2^n-1\}$ *such that* $\{0,\ldots,2^t-1\}\} \subseteq A_1$ *and* $A_2 \subseteq \{0,\cdots,2^n-1\}$ *such that* $\{2^t x : x \in \{0,\ldots,2^{n-t}-1\}\} \subseteq A_2$. *Putting* $\gamma = 1 - \log(3)(1/2+\delta_1)$ *we obtain:*

$$(\ell-1)/2 \geq \sharp S_1 \geq (\ell-1)^{(1/2+\delta_1)} \quad \textit{and} \quad \sharp S_2 \geq (\ell-1)/2+1,$$

for all but at most $3/2(\ell-1)^{n-\gamma} + (\ell-1)^{n-\delta_2}$ *vectors* $\mathbf{a} \in (\mathbb{F}_\ell^*)^n$.

We then apply Lemma 9 to Theorem 6 to obtain the following corollary:

Corollary 3 *Let* $\frac{1}{\log(3)} - \frac{1}{2} > \delta_1 > 0$, $\delta_2 > 0$ *and* $\gamma = 1 - \log(3)(1/2+\delta_1)$. *Let* t *and* n *be integers such that* $t = \lceil (1/2+\delta_1)\log(\ell-1)\rceil + s$ *for some integer* s *such that* $0 \leq s \leq \log(\ell-1) - 1 - \lceil (1/2+\delta_1)\log(\ell-1)\rceil$ *and* $n - t \geq (1+\delta_2)\log(\ell-1)+2$. *Let* $A_1 \subseteq \{0,\cdots,2^n-1\}$ *such that* $\{0,\ldots,2^t-1\}\} \subseteq A_1$ *and* $A_2 \subseteq \{0,\cdots,2^n-1\}$ *such that* $\{2^t x : x \in \{0,\ldots,2^{n-t}-1\}\} \subseteq A_2$. *For some* $\mathbf{a} \in (\mathbb{F}_\ell^*)^n$, *let* $F_{\mathbf{a}}(X,Y) \in \mathbb{F}_p[X,Y]$ *such that*

$$F_{\mathbf{a}}(f_{\mathbf{a}}(x), f_{\mathbf{a}}(x')) = f_{\mathbf{a}}(x+x') \tag{9}$$

for all $(x,x') \in A_1 \times A_2$. *We have*

$$\deg(F_{\mathbf{a}}) \geq (\ell-1)^{(1/2+\delta_1)}/8,$$

for all but at most $3/2(\ell-1)^{n-\gamma} + (\ell-1)^{n-\delta_2}$ *vectors* $\mathbf{a} \in (\mathbb{F}_\ell^*)^n$.

The proof is straightforward since, with the notation of Theorem 6, we have in this case $\sharp S_1 \geq (\ell-1)^{(1/2+\delta_1)}$ and there exists $v \in S_2$ such that $2v \in S_2$ since $\sharp S_2 > (\ell-1)/2$

6 Conclusion

In this paper, we proved lower bounds on the degree of multivariate polynomial representations of the Naor-Reingold function over a finite field and over the group of points on an elliptic curve over a finite field. Many open problems remain: the first being naturally to generalize our bounds to smaller interpolating sets. Known lower bounds on the polynomial interpolation of the

Diffie-Hellman mapping (*e.g.* [9,7,13,22])) can rule out the existence of low degree polynomials that interpolate the Naor-Reingold function in two fixed points for many keys. It is desirable to extend these results to give lower bounds on the degree of general multivariate polynomials that interpolate the Naor-Reingold function in several fixed points for many keys. Such results would be related to the polynomial interpolation of the so-called *group Diffie-Hellman* problems [3].

Acknowledgements. The authors would like to thank the anonymous reviewers for their helpful and constructive comments that led to substantial improvements in this paper.

References

1. Banks, W.D., Griffin, F., Lieman, D., Shparlinski, I.: Non-linear complexity of the Naor-Reingold pseudo-random function. In: J. Song (ed.) ICISC 99: 2nd International Conference on Information Security and Cryptology, *Lecture Notes in Computer Science*, vol. 1787, pp. 53–59. Springer, Heidelberg, Germany, Seoul, Korea (2000)
2. Blake, I.F., Seroussi, G., Smart, N.P.: Elliptic curves in cryptography. Cambridge: Cambridge University Press (1999)
3. Bresson, E., Chevassut, O., Pointcheval, D.: The group Diffie-Hellman problems. In: K. Nyberg, H.M. Heys (eds.) SAC 2002: 9th Annual International Workshop on Selected Areas in Cryptography, *Lecture Notes in Computer Science*, vol. 2595, pp. 325–338. Springer, Heidelberg, Germany, St. John's, Newfoundland, Canada (2003)
4. Coppersmith, D., Shparlinski, I.: On polynomial approximation of the discrete logarithm and the Diffie-Hellman mapping. Journal of Cryptology **13**(3), 339–360 (2000)
5. Cruz, M., Gómez, D., Sadornil, D.: On the linear complexity of the Naor-Reingold sequence with elliptic curves. Finite Fields Appl. **16**(5), 329–333 (2010)
6. Domingo Gmez, J.G., lvar Ibeasi: On the linear complexity of the Naor-Reingold pseudo-random function. Inf. Process. Lett. **111**, 854–856 (2011)
7. El Mahassni, E., Shparlinski, I.: Polynomial representations of the Diffie-Hellman mapping. Bull. Aust. Math. Soc. **63**(3), 467–473 (2001)
8. Griffin, F., Shparlinski, I.E. (eds.): On the linear complexity of the Naor-Reingold pseudo-random number generator, Proc. 2nd Intern. Conf. on Information and Communication Security, ICICS1999, Sydney, *Lecture Notes in Computer Science*, vol. 1726. Springe-Verlag, Berlin (1999)
9. Kiltz, E., Winterhof, A.: On the interpolation of bivariate polynomials related to the Diffie-Hellman mapping. Bull. Aust. Math. Soc. **69**(2), 305–315 (2004)
10. Kiltz, E., Winterhof, A.: Polynomial interpolation of cryptographic functions related to Diffie-Hellman and discrete logarithm problem. Discrete Appl. Math. **154**(2), 326–336 (2006)
11. Lange, T., Winterhof, A.: Polynomial interpolation of the elliptic curve and XTR discrete logarithm. In: O.H. Ibarra, L. Zhang (eds.) Computing and Combinatorics, 8th Annual International Conference, COCOON 2002, Singapore, August 15-17, 2002, Proceedings, *Lecture Notes in Computer Science*, vol. 2387, pp. 137–143. Springer (2002)
12. Lange, T., Winterhof, A.: Interpolation of the discrete logarithm in $\mathbb{F}_q$ by Boolean functions and by polynomials in several variables modulo a divisor of $q-1$. Discrete Appl. Math. **128**(1), 193–206 (2003)
13. Lange, T., Winterhof, A.: Interpolation of the elliptic curve Diffie-Hellman mapping. In: M.P.C. Fossorier, T. Høholdt, A. Poli (eds.) Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, 15th International Symposium, AAECC-15, Toulouse, France, May 12-16, 2003, Proceedings, *Lecture Notes in Computer Science*, vol. 2643, pp. 51–60. Springer (2003)

14. Ling, S., Shparlinski, I.E., Wang, H.: On the multidimensional distribution of the Naor-Reingold pseudo-random function. Math. Comput. **83**(289) (2014)
15. Meletiou, G.C., Winterhof, A.: Interpolation of the double discrete logarithm. In: J. von zur Gathen, J.L. Imaña, Ç.K. Koç (eds.) Arithmetic of Finite Fields, 2nd International Workshop, WAIFI 2008, Siena, Italy, July 6-9, 2008, Proceedings, *Lecture Notes in Computer Science*, vol. 5130, pp. 1–10. Springer (2008)
16. Naor, M., Reingold, O.: Number-theoretic constructions of efficient pseudo-random functions. In: 38th Annual Symposium on Foundations of Computer Science, pp. 458–467. IEEE Computer Society Press, Miami Beach, Florida (1997)
17. Naor, M., Reingold, O.: Number-theoretic constructions of efficient pseudo-random functions. J. ACM **51**(2), 231–262 (2004)
18. Shparlinski, I.E.: Linear complexity of the Naor-Reingold pseudo-random function. Inf. Process. Lett. **76**(3), 95–99 (2000)
19. Shparlinski, I.E.: On the Naor-Reingold pseudo-random function from elliptic curves. Appl. Algebra Eng. Commun. Comput. **11**(1), 27–34 (2000)
20. Shparlinski, I.E., Silverman, J.H.: On the linear complexity of the Naor-Reingold pseudo-random function from elliptic curves. Des. Codes Cryptography **24**(3), 279–289 (2001)
21. Washington, L.C.: Elliptic curves. Number theory and cryptography. 2nd ed., 2nd ed. edn. Boca Raton, FL: Chapman and Hall/CRC (2008)
22. Winterhof, A.: A note on the interpolation of the Diffie-Hellman mapping. Bull. Aust. Math. Soc. **64**(3), 475–477 (2001)